明 細 書

暗号方式の安全性を保証するパディング適用方法

化装置

技術分野

[0001] 本発明は情報の暗号化／復号化システムに係り、特に選択暗号文攻撃に対し安全性を保証するパディング適用方法および暗号化／復号化装置に関する。

背景技術

[0002] 通信のセキュリティを確保するために暗号技術の社会的応用が盛んに進められ、効率的な暗号計算が従来以上に望まれている。このような傾向のなかで、Jeffrey Hoffstein、Jill PipherおよびJoseph H. Silvermanによる文献"NTRU:A Ring-Based Public Key Cryptosystem"（非特許文献1）により提案されたNTRU暗号方式は、従来のRSA暗号方式やElGamal暗号方式と比べ、メモリ消費が少なく高速な暗号／復号計算方法として注目されている。

[0003] （NTRU暗号化方式）

NTRU暗号方式は以下のような公開鍵暗号方式である。

[0004] まず以下のようにして鍵生成を行う。正整数p, q, Nをとり領域変数として公開し、$R = Z[X]/(X^N-1)$とする。以下、L(a,b)は、Rの元uであって、uの各次数の係数のうちa個が1でb個が-1、他のものが0であるもの全体の集合（Rの部分集合）を表すものとする。パラメータdf, dg, dを決め、$L_f = L(df, df+1)$, $Lg = L(dg, dg+1)$, $L\phi = L(d, d)$とする。L_fからfを、L_gからgをランダムに取り、$h = f^{-1}g \bmod q$とする。f, gを秘密鍵とし、hを公開鍵とする。

[0005] 鍵が生成されると、Rの部分集合L_mの元mを暗号化する。まず、Rの部分集合元L_rからr をランダムに選び、$e = phr + m \bmod q$ を計算し、eを暗号文として出力する。

[0006] 暗号文eから元の平文mを復号するには、まず$fe = pgr + fm \bmod q$を計算する。f, g, r, mがそれぞれL_f、L_g、L_r、L_mの元であることから $fe = pgr + fm$であるので、$fe \pmod p = m \pmod p$を計算することができ、mがL_mの元であることから$m = m \pmod p$なので m を復元できる。

[0007] しかしながら、Don Coppersmith、Adi Shamirによる文献“Lattice Attacks on NTRU”, Eurocrypt'97 Springer Lecture Notes in Computer Sciences,1997(非特許文献2)などに指摘されているように、NTRU暗号方式には数々の解読方法が知られている。これに対して、平文に何らかのパディングを施した後、NTRU暗号化することにより解読を防御する方法が幾つか知られている。

[0008] (OAEP+パディング方式)

暗号方式を安全にするためのパディング方法としては、例えばVictor Shoupによる文献“OAEP Reconsidered”Journal of Cryptology 15(4)(非特許文献3)で提案されたOAEP+と呼ばれるパディング方法が知られている。OAEP+パディングは以下のようなパディング方式である。

[0009] まず、パラメータk, k_0, k_1を次のように選ぶ:k, k_0, k_1は正整数、かつ、$k_0 + k_1 \leqq k \leqq L$を満たす。ここで、Lは平文空間の元の数である。

[0010] さらに、$n = k - k_0 - k_1$とし、

Gは、kビットのビット列にnビットのビット列を対応させるハッシュ関数、

H'は、$n+k_0$ビットのビット列にk_1ビットのビット列を対応させるハッシュ関数、および、

Hは、$n+k_1$ビットのビット列にk_0ビットのビット列を対応させるハッシュ関数とする。

[0011] パディング装置はnビットの平文Mを受け取り、k_0ビットのビット列Rをランダムに選ぶ。続いて、G(R)とMのビット毎の排他的論理和s^0を計算し、s^1=H'(R||M)を計算し、$s = s^0 || s^1$とする。ここで「||」はビット列の連接を表す。tをH(s)とRのビット毎の排他的論理和とし、w = s||tとする。このwを「平文Mの乱数Rを用いたOAEP+パディング」と呼ぶ。こうして得られたOAEP+パディングwを(乱数を使わない暗号方式で)暗号化し、暗号文eを受信者に送信する。

[0012] 受信者は、受信した暗号文eを復号し、wを得る。wを復号後、パディング復元装置は以下のようにして平文Mを復元する。まずwは$w = s||t = s_0||s_1||t$の形をしているので、これを使ってs_0、s_1、tを復元する。次にH(s)とtのビット毎の排他的論理和を取ることによりRを復元する。G(R)とs_0のビット毎の排他的論理和を計算することによりMを復元する。s_1 = H'(R||M)を満たせばMを出力し、満たさなければeは不正な暗号文として「⊥」を出力する。

[0013] しかしながら、このOAEP+パディングは、暗号化関数を計算する際に乱数を使用しない暗号方式に対して適応するために提案されたパディング方式である。このために、上述したNTRUのような乱数を使用した暗号方式に適応した場合は必ずしも安全性が保証されないという問題がある。また、NTRUのような乱数を使用した暗号方式にOAEP+パディングを適応する場合には、適応方法は一意ではなく様々な方法を考えることができるために、どのようなパディングの適用方法が安全で、どのようなパディングの適用方法が安全でないかがすぐには分からないという問題もある。

[0014] このようにOAEP+パディング方式は乱数を使用しない暗号方式に対してのみ安全性が保証できるのであるが、乱数を使用するNTRU暗号方式に対してOAEP+パディング方式ないしそれに類似したパディング方式を適応することで安全性を保証しようという試みもいくつか提案されている。たとえば、次の文献を参照されたい。

[0015] ・Joseph H. Silvermanによる文献"Plaintext Awareness and the NTRU PKCS" Technical Report#7 version 2, NTRU Cryptosystems, 1998(非特許文献4)

・Jeffrey Hoffstein、Joseph H. Silvermanによる文献"Optimizations for NTRU" Public-key Cryptography and Computational Number Theory(非特許文献5)

・Jeffrey Hoffstein、Joseph H. Silvermanによる文献"Protecting NTRU Against Chosen Ciphertext and Reaction Attacks"Technical Report, NTRU Cryptosystems, 2000, Report#16 version 1(非特許文献6)

・Phong Q. Nguyen、David Pointchevalによる文献"Analysis and Improvements of NTRU Encryption Paddings"Crypto 2002 Springer Lecture Notes in Computer Sciences, 2002(非特許文献7)。

[0016] しかしながら、これらのパディングつきNTRU暗号方式はすべて解読された。非特許文献4に記載されたパディングを施したNTRU暗号方式は、Eliane Jaulmes、Antoine Jouxによる文献"A Chosen-Ciphertext Attack against NTRU"Crypto 2000 Springer Lecture Notes in Computer Sciences, 2000(非特許文献8)で提案されたアルゴリズムで解読された。

[0017] また、非特許文献5および6に記載されたパディングを施したNTRU暗号方式は非特許文献7で提案されたアルゴリズムで解読され、この非特許文献7によるパディング

方法はJohn A. Proosによる"Imperfect Decryption and an Attack on the NTRU Encryption Scheme"(非特許文献9)により解読された。

[0018] OAEP+パディング方式以外のパディング方式を用いてNTRU暗号方式のような乱数を使った暗号方式の安全性確保を図った方式も提案されているが、パディング方式は方式毎に異なる弱点を持っているために、OAEP+パディングを用いて暗号方式の安全性を確保することは依然として有意義である。

非特許文献1:Jeffrey Hoffstein、Jill PipherおよびJoseph H. Silvermanによる文献" NTRU:A Ring-Based Public Key Cryptosystem"

非特許文献2:"Lattice Attacks on NTRU", Eurocrypt'97 Springer Lecture Notes in Computer Sciences,1997

非特許文献3:"OAEP Reconsidered"Journal of Cryptology 15(4)

非特許文献4:"Plaintext Awareness and the NTRU PKCS" Technical Report#7 version 2, NTRU Cryptosystems, 1998

非特許文献5:Jeffrey Hoffstein、Joseph H. Silvermanによる文献"Optimizations for NTRU" Public-key Cryptography and Computational Number Theory

非特許文献6:"Protecting NTRU Against Chosen Ciphertext and Reaction Attacks" Technical Report, NTRU Cryptosystems, 2000, Report#16 version 1

非特許文献7:"Analysis and Improvements of NTRU Encryption Paddings"Crypto 2002 Springer Lecture Notes in Computer Sciences, 2002

非特許文献8:"A Chosen-Ciphertext Attack against NTRU"Crypto 2000 Springer Lecture Notes in Computer Sciences, 2000

非特許文献9:John A. Proosによる"Imperfect Decryption and an Attack on the NTRU Encryption Scheme"

発明の開示

発明が解決しようとする課題

[0019] 上述したように、従来のパディングつきNTRU暗号方式は安全な暗号通信を行うことができない。

[0020] 本発明の目的はNTRU暗号方式のような方式に対して適切なパディングを施すこと

で安全な暗号通信を達成するパディング適用方法および暗号化／復号化装置を提供することにある。

課題を解決するための手段

[0021] 本発明者は、NTRU暗号方式では暗号に使用した乱数を復元可能であることに着目し、暗号通信の安全性を保証できる新規なパディング適用方式を発明した。

[0022] (成立根拠)

まず、本発明の成立根拠について簡単に説明する。乱数を使用した暗号方式で代表的なものに、エルガマル暗号方式やペイリエー暗号方式などがある。これらの暗号方式では、暗号文受信者が平文を復元することはできるが乱数を復元することはできないために、平文と乱数とは全く異なる種類のデータとして扱う必要がある。

[0023] また、エルガマル暗号方式やペイリエー暗号方式等の多くの暗号方式では、暗号化関数は確率的な関数であり、暗号化関数の定義域は平文M全体の空間であり、値域は暗号文全体の空間である。それに対し、復号化関数は確率を使わない関数であり、定義域は暗号文全体の空間で値域は平文全体の空間である。繰り返すが、これらの暗号方式では暗号に使用した乱数を復元できない。

[0024] これに対して、NTRU暗号方式は、平文mを復元した後に、$r = (fe - fm)/pg$ により乱数rを求めることができる、という特徴がある。このため、NTRU暗号方式は、エルガマル暗号方式やペイリエー暗号方式等の暗号方式とは異なり、平文と乱数とを区別する必然性がない。

[0025] したがって、NTRU暗号方式では、次のようにみなすことができる。

[0026] ・暗号化関数は乱数を使わない関数であり、その定義域は平文Mと乱数Rとの連接全体の空間、値域は暗号文全体の空間である。

[0027] ・復号化関数も乱数を使わない関数であり、その定義域は暗号文全体の空間、値域は平文Mと乱数Rとの連接全体の空間である。

[0028] 既に述べたようにOAEP+パディングは暗号化関数が乱数を使わない場合には安全性が保証される。したがって、NTRU暗号方式の平文と乱数とを区別しないデータ構造に対して、安全性保証つきOAEP+パディングを適用可能であることがわかる。

[0029] (本発明の概要)

この知見に基づいて、本発明がなされた。すなわち、本発明によるパディング適用方式は、暗号文作成者が暗号文の作成に使用した乱数の値を暗号文受信者が復元できる暗号方式$E^r(m)$に対して適用可能であり、このような暗号方式に対して本発明を適用した場合に安全性が保証される。

[0030] 本発明によれば、暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用する方法は、入力情報を前記パディング方式により所定長以下のビット列に変換し、前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換し、前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給し、前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、ことを特徴とする。

[0031] 本発明の一実施形態によれば、変換規則は、前記ビット列の前半を前記第1ビット列とし、後半を前記第2ビット列とするように前記ビット列を2分割する規則である。

[0032] 本発明の一実施例によれば前記パディング方式はOAEP＋パディングであり、前記乱数を使用する暗号化方式はNTRU暗号方式である。

[0033] 図1(A)は、本発明によるパディング適用方式による暗号化装置の概念的ブロック図であり、(B)は従来例によるOAEPベースのパディング方式を適用した暗号化装置の概念的ブロック図である。ただし、パラメータは最も標準的な場合が示されており、$n = k_0 = k_1$であり、mのビット数はrである。

[0034] 図1(A)を用いて本発明によるパディング適用方式を説明すると、おおよそ次のようになる。まず、OAEP+パディング方式と同様のパラメータを選ぶ。すなわち、上述したように、正整数k, k_0, k_1を$k_0 + k_1 < k < L$を満たすように取る。ここでLは平文空間の元の数である。$n = k - k_0 - k_1$とし、Gをkビットのビット列にnビットのビット列を対応させるハッシュ関数、H'を$n+k_0$ビットのビット列にk_1ビットのビット列を対応させるハッシュ関数、Hを$n+k_1$ビットのビット列にk_0ビットのビット列を対応させるハッシュ関数とする。

[0035] 次に、nビットの平文Mを受け取り、OAEP+パディングを行う。すなわちk_0ビットのビット列Rをランダムに選び、G(R)とMのビット毎の排他的論理和s^0を計算し、s^1=H'(R||M)を計算して、$s = s^0||s^1$とする。記号「||」はビット列の連接を表す。tをH(s)とRのビット毎の排他的論理和とし、w = s||tとする。

[0036] 次に、wを次の条件を満たす規則A(以下、変換関数Aという。)を用いて2つのビット列mおよびrを生成する。Aは、kビット以下のビット列に$L_m \times L_r$の元を対応させる写像であり、ここでL_mはmの取りうる範囲、L_rはrの取りうる範囲である。変換関数Aが満たすべき条件は次の通りである。

[0037] (1)Aは単射であること

(2)Aおよびその逆写像は多項式時間で計算できること

(3)暗号化関数をE(m,r)とした時、写像E:A(X)→L_eは、一方向性関数であること(ただしXは(m,r)の取りうる範囲を表し、L_eは暗号文全体の空間を表す)。

[0038] NTRU暗号方式の場合、例えばビット列wを前半のビット列と後半のビット列に等分割して、それぞれをmおよびrとすればよい。こうして2つのビット列に変換されると、$e = E^r(m)$を計算して暗号化し、eを暗号文受信者に送信する。

[0039] 受信者はeを受信したら、eを復号してmを得る。上述したように$E^r(m)$の特徴によりrは復元可能であるから、rを復元する。そして、w = m||rによりwを復元する。wを復号後、OAEP+パディングの復元と同様にMを復元する。具体的には、まず、wはw = s||t =s_0||s_1||tの形をしているので、これを使ってs_0、s_1、tを復元する。次に、H(s)とtのビット毎の排他的論理和を取ることによりRを復元し、G(R)とs_0のビット毎の排他的論理和を計算することによりMを復元する。s_1 = H'(R||M)を満たせば、Mを出力し、そうでなければeは不正な暗号文として⊥を出力する。

発明の効果

[0040] 次に、本発明による方式と従来の方式とを比較して、本発明の効果を説明する。図1(B)に一例を示すように、上述した非特許文献4ー7で提案された方式では、平文MからOAEP+(あるいはその他の)パディング方式を使ってmのみを作り上げ、rは何らかの別の手段を用いて作っている。これらの方式は、エルガマル暗号方式やペイリエー暗号方式のような受信側で平文だけが復元でき乱数は復元できない暗号方式に

対しても利用できるが、ad-hocな方法であるため安全性が保証できず、特にNTRUの場合には完全解読が可能である。

[0041] これに対して、本発明による方式は、NTRUのような暗号文受信者が平文および乱数を共に復元できる暗号方式に適用されるパディング方式である。上記の従来の方式とは異なり、平文MからOAEP+パディング方式および所定の変換規則(関数A)を使ってmおよびrの両方を作り上げる。また、従来の方式とは異なり、NTRUのような暗号文受信者が平文および乱数をともに復元できる暗号方式に対して適用した場合に安全性が保証できる。

[0042] すなわち、本発明により、NTRU暗号方式という必要メモリ量の少なくかつ暗号化復号化計算が高速な暗号方式を利用して安全な暗号通信を行うことが可能になる。

発明を実施するための最良の形態

[0043] 図2は、本発明による暗号化／復号化装置を実装した暗号通信システムの一例を示すブロック図である。ここではネットワークを通して通信端末間で暗号通信が行われる。

[0044] 送信側の通信端末は、プログラム制御プロセッサ10、乱数生成器11、プログラムメモリ12、メモリ13および送受信部14を有し、後述するように、プログラムメモリ12に格納されたOAEP＋変換、変換関数Aによる変換、NTRU暗号化などの必要なプログラムを実行することで平文を暗号化し、暗号文を送受信部14からネットワークを通して宛先の受信端末へ送信する。なお、メモリ13には、公開情報や秘密鍵などの暗号化に必要な情報が格納されている。

[0045] 受信端末も同様に、プログラム制御プロセッサ20、乱数生成器21、プログラムメモリ22、メモリ23および送受信部24を有し、後述するように、プログラムメモリ22、メモリ13および送受信部14を有し、後述するように、プログラムメモリ22に格納されたNTRU復号化、乱数復元、逆変換、OAEP＋逆変換などの必要なプログラムを実行することで、送受信部24で受信した暗号文を平文に復号する。なお、メモリ23には、公開情報や秘密鍵などの復号化に必要な情報が格納されている。

[0046] 1. 第1実施形態

図3は、本発明の第1実施形態による暗号化／復号化装置の機能的構成を示すブ

ロック図である。本実施形態による暗号化／復号化装置は、平文を暗号化するための暗号化装置100と、暗号文を平文に復号するための復号化装置200とを有し、さらに鍵生成装置300により生成された暗号化／復号化に必要な公開情報を記憶する公開情報記憶装置301、復号化に必要な秘密鍵情報を記憶する秘密鍵記憶装置302を有する。

[0047] 平文は、平文入力装置101により暗号化装置100へ与えられ、暗号化装置100にはOAEP+変換部102、変換関数Aによる変換部103およびNTRU暗号化部104などのプロセスが実現されている。暗号化装置100により生成された暗号文は暗号文出力装置105を通して、例えば受信端末へ出力される。

[0048] 暗号文は、暗号文入力装置201により復号化装置200へ与えられ、復号化装置200にはNTRU復号化部202、乱数復元部203、変換関数Aの逆変換部204、OAEP+逆変換部205などのプロセスが実現されている。復号化装置200により生成された平文は平文出力装置206を通して出力される。

[0049] 1．1)鍵生成

まず鍵生成手順を説明する。

[0050] 図4は、第1実施形態における鍵生成手順を示すフローチャートである。鍵生成装置300は、正整数p, q, Nをとり、領域変数として公開する。上述したNTRU暗号方式と同様に、$R = Z[X]/(X^N-1)$とし、Rの元uであってuの各次数の係数のうちa個が1でb個が−1、他のものが0であるもの全体の集合（Rの部分集合）をL(a,b)で表すものとし、Rの部分集合L_f, L_g, L_r, L_mを取る（ステップS11）。

[0051] さらに鍵生成装置1は、OAEP+パディング方式で説明したように、パラメータk, k_0, k_1を次のように選ぶ：k, k_0, k_1は正整数、かつ、$k_0 + k_1 \leqq k \leqq L$を満たす。ここで、Lは$L_m \times L_r$の元の数である。さらに、$n = k - k_0 - k_1$とし、

Gは、kビットのビット列にnビットのビット列を対応させるハッシュ関数、

H'は、$n+k_0$ビットのビット列にk_1ビットのビット列を対応させるハッシュ関数、および、

Hは、$n+k_1$ビットのビット列にk_0ビットのビット列を対応させるハッシュ関数とする（ステップS12）。

[0052] さらに、鍵生成装置1は変換関数Aを決定する（ステップS13）。変換関数Aはkビッ

ト以下のビット列に$L_m \times L_r$の元を対応させる写像とし、以下の性質を満たさねばならない。

[0053] (1)Aは単射であること

(2)Aおよびその逆写像が多項式時間で計算できること

(3)暗号化関数をE(m, r)とした時、写像E:A(X)→L_eは、一方向性関数であること(ただし、Xは(m, r)の取りうる範囲を表し、L_eは暗号文全体の空間を表す)。

[0054] 鍵生成装置1は、NTRUと同様の方法で鍵生成を実行する。すなわちL_fからfを、L_gからgをランダムに取り、$h = f^{-1}g \bmod q$とする。f, gを秘密鍵とし、hを公開鍵とする(ステップS14)。鍵生成装置1は、f, gを秘密鍵記憶装置302に秘密裡に保持し(ステップS15)、NTRUの公開鍵、上記ハッシュ関数および変換関数(p, q, N, L_f, L_g, L_r, L_m, k, k_0, k_1, G, H', H, A, h)を公開情報記憶装置301に格納して公開する(ステップS16)。

[0055] 1. 2)暗号化手順

次に暗号化手順を説明する。

[0056] 図5は、第1実施形態における暗号化手順を示すフローチャートである。暗号化装置100は、まず平文入力装置101からnビットの平文Mを受け取り(ステップS21)、公開情報記憶装置301から公開情報p, q, N, L_f, L_g, L_r, L_m, k, k_0, k_1, G, H', H, A, およびhを受け取る(ステップS22)。

[0057] 続いて、k_0ビットのビット列Rをランダムに選び(ステップS23)、OAEP+変換部102は、G(R)とMのビット毎の排他的論理和s^0を計算し、s^1=H'(R||M)を計算し、$s = s^0||s^1$とし、さらに、tをH(s)とRのビット毎の排他的論理和として、w = s||tを生成することで、平文をOAEP+パディングする(ステップS24)。

[0058] さらに、変換部103は変換関数Aを用いて、(m, r)=A(w)によって、wを2つのビット列mおよびrに変換する(ステップS25)。ここでは、wを等分割して前半のビット列をm、後半のビット列をrとする。そして、NTRU暗号化部104は、$e = phr + m \bmod q$を計算することでNTRU暗号化を行い(ステップS26)、生成された暗号文を暗号文出力装置105から出力する(ステップS27)。

[0059] 1. 3)復号化手順

最後に復号化手順を説明する。

[0060] 図6は、第1実施形態における復号化手順を示すフローチャートである。まず復号化装置200は暗号文入力装置201から暗号文eを受け取り(ステップS31)、続いて、秘密鍵記憶装置302から暗号文に対応する秘密鍵を、公開情報記憶装置301からその秘密鍵に対応する公開情報を受け取る(ステップS32)。

[0061] NTRU復号部202は、公開情報および秘密鍵を用いて、NTRU暗号方式と同様に暗号文eの復号化処理を行う。すなわち、fe = pgr + fm mod qを計算し、f, g, r, mがそれぞれL_f、L_g、L_r、L_mの元であることからfe = pgr + fmであるので、fe (mod p) = m (mod p)を計算することができ、mがL_mの元であることからm = m (mod p)なので、mを復元できる(ステップS33)。

[0062] また、乱数復元部203は、fe = pgr + fmであるので、r = (fe − fm)/pgによりrを復元する(ステップS34)。

[0063] 次に、逆変換部204は変換関数Aの逆変換を用いて、$A^{-1}(m,r)$により、w = s||t = s_0||s_1||tを復元する(ステップS35)。続いて、OAEP+逆変換部205は、H(s)とtのビット毎の排他的論理和を取ることによりRを復元し、G(R)とs_0のビット毎の排他的論理和を計算することによりMを復元する(ステップS36)。

[0064] 最後に、パディングが正当であるか否かをs_1 = H'(R||M)が満たされるか否かによって判断し(ステップS37)、正当であれば平文Mを出力し(ステップS38)、正当でなければ暗号文eは不正な暗号文として⊥を出力する(ステップS39)。

[0065] 2. 第2実施形態

図7は、本発明の第2実施形態による暗号化／復号化装置の機能的構成を示すブロック図である。本実施形態による暗号化／復号化装置は、平文を暗号化するための暗号化装置400と、暗号文を平文に復号するための復号化装置500とを有し、さらに鍵生成装置300により生成された暗号化／復号化に必要な公開情報を記憶する公開情報記憶装置301、復号化に必要な秘密鍵情報を記憶する秘密鍵記憶装置302を有する。

[0066] 平文は、平文入力装置101により暗号化装置400へ与えられ、暗号化装置400には乱数発生部401、秘密鍵暗号化部402、OAEP+変換部403、変換関数Aによる変

換部404およびNTRU暗号化部405などのプロセスが実現されている。暗号化装置400により生成された暗号文は暗号文出力装置105を通して、例えば受信端末へ出力される。

[0067] 暗号文は、暗号文入力装置201により復号化装置500へ与えられ、復号化装置500にはNTRU復号化部501、乱数復元部502、変換関数Aの逆変換部503、OAEP+逆変換部504、秘密鍵暗号復号部505などのプロセスが実現されている。復号化装置500により生成された平文は平文出力装置206を通して出力される。

[0068] 2. 1)鍵生成

まず鍵生成手順を説明する。

[0069] 図8は、第2実施形態における鍵生成手順を示すフローチャートである。鍵生成装置300は、正整数p, q, Nをとり、領域変数として公開する。上述したNTRU暗号方式と同様に、$R = Z[X]/(X^N-1)$とし、Rの元uであってuの各次数の係数のうちa個が1でb個が-1、他のものが0であるもの全体の集合(Rの部分集合)をL(a,b)で表すものとし、Rの部分集合L_f, L_g, L_r, L_mを取る(ステップS41)。

[0070] さらに鍵生成装置1は、OAEP+パディング方式で説明したように、パラメータk, k_0, k_1を次のように選ぶ:k, k_0, k_1は正整数、かつ、$k_0 + k_1 \leqq k \leqq L$を満たす。ここで、Lは$L_m \times L_r$の元の数である。さらに、$n = k - k_0 - k_1$とし、

Gは、kビットのビット列にnビットのビット列を対応させるハッシュ関数、

H'は、$n+k_0$ビットのビット列にk_1ビットのビット列を対応させるハッシュ関数、および、

Hは、$n+k_1$ビットのビット列にk_0ビットのビット列を対応させるハッシュ関数とする(ステップS42)。

[0071] さらに、鍵生成装置1は変換関数Aを決定する(ステップS43)。変換関数Aは、上述したように、kビット以下のビット列に$L_m \times L_r$の元を対応させる写像とし、以下の性質を満たさねばならない。

[0072] (1)Aは単射であること

(2)Aおよびその逆写像が多項式時間で計算できること

(3)暗号化関数をE(m, r)とした時、写像$E:A(X) \rightarrow L_e$は、一方向性関数であること(ただし、Xは(m, r)の取りうる範囲を表し、L_eは暗号文全体の空間を表す)。

[0073] 鍵生成装置1は、NTRUと同様の方法で鍵生成を実行する。すなわちL_fからfを、L_gからgをランダムに取り、$h = f^{-1}g \bmod q$とする。f, gを秘密鍵とし、hを公開鍵とする。鍵生成装置1は、f, gを秘密鍵記憶装置302に秘密裡に保持し(ステップS44)する。

[0074] さらに、鍵生成装置1は、使用する共通鍵鍵暗号方式Eを決定し(ステップS45)、NTRUの公開鍵、上記ハッシュ関数および変換関数(p, q, N, L_f, L_g, L_r, L_m, k, k_0, k_1, G, H', H, A, h)を公開情報記憶装置301に格納して公開する(ステップS46)。

[0075] 2. 2)暗号化手順

次に暗号化手順を説明する。

[0076] 図9は、第2実施形態における暗号化手順を示すフローチャートである。暗号化装置400は、まず平文入力装置101からnビットの平文Xを受け取り(ステップS51)、公開情報記憶装置301から公開情報p, q, N, L_f, L_g, L_r, L_m, k, k_0, k_1, G, H', H, A,およびhを受け取る(ステップS52)。

[0077] 続いて、乱数発生部401を用いて秘密鍵暗号化部402はnビットのビット列Mをランダムに選び(ステップS53)、$Y = E_M(X)$を計算して共通化鍵暗号化を行う(ステップS54)。ここで、$E_M(X)$は、Mを鍵として平文Xを共通鍵暗号方式Eに従って暗号化したものである。

[0078] 続いて、k_0ビットのビット列Rをランダムに選び(ステップS55)、OAEP+変換部403は、G(R)とMのビット毎の排他的論理和s^0を計算し、s^1=H'(R||M)を計算し、$s = s^0||s^1$とし、さらに、tをH(s)とRのビット毎の排他的論理和として、w = s||tを生成することで、平文をOAEP+パディングする(ステップS56)。

[0079] さらに、変換関数Aによる変換部404は、(m, r) = A(w)によってwを2つのビット列mおよびrに変換する(ステップS57)。ここでは、wを2分割して前半のビット列をm、後半のビット列をrとする。そして、NTRU暗号化部405は、$e = phr + m \bmod q$を計算することでNTRU暗号化を行い(ステップS58)、生成された暗号文eと共通鍵暗号の暗号文Yとを暗号文(e, Y)として暗号文出力装置105から出力する(ステップS59)。

[0080] 2. 3)復号化手順

最後に復号化手順を説明する。

[0081] 図10は、第2実施形態における復号化手順を示すフローチャートである。まず復号

化装置500は暗号文入力装置201から暗号文eを受け取り(ステップS61)、続いて、秘密鍵記憶装置302から暗号文に対応する秘密鍵を、公開情報記憶装置301からその秘密鍵に対応する公開情報を受け取る(ステップS62)。

[0082] NTRU復号化部501は、公開情報および秘密鍵を用いて、NTRU暗号方式と同様に暗号文eの復号化処理を行う。すなわち、$fe = pgr + fm \bmod q$を計算し、f, g, r, mがそれぞれL_f、L_g、L_r、L_mの元であることから$fe = pgr + fm$であるので、$fe \pmod p = m \pmod p$を計算することができ、mがL_mの元であることから$m = m \pmod p$なので、mを復元できる(ステップS63)。

[0083] また、乱数復元部502は、$fe = pgr + fm$であるので、$r = (fe - fm)/pg$によりrを復元する(ステップS64)。

[0084] 次に、逆変換部503は、$A^{-1}(m,r)$により、$w = s\|t = s_0\|s_1\|t$を復元する(ステップS65)。続いて、OAEP+逆変換部504は、H(s)とtのビット毎の排他的論理和を取ることによりRを復元し、G(R)とs_0のビット毎の排他的論理和を計算することによりMを復元する(ステップS66)。

[0085] 最後に、パディングが正当であるか否かを$s_1 = H'(R\|M)$が満たされるか否かによって判断し(ステップS67)、正当であれば、共通鍵暗号の鍵Mを用いて共通鍵暗号を解き、平文Xを出力し(ステップS68)、正当でなければ暗号文eは不正な暗号文として⊥を出力する(ステップS69)。

図面の簡単な説明

[0086] [図1](A)は、本発明によるパディング適用方式による暗号化装置の概念的ブロック図であり、(B)は従来例によるOAEPベースのパディング方式を適用した暗号化装置の概念的ブロック図である。

[図2]本発明による暗号化／復号化装置を実装した暗号通信システムの一例を示すブロック図である。

[図3]本発明の第1実施形態による暗号化／復号化装置の機能的構成を示すブロック図である。

[図4]第1実施形態における鍵生成手順を示すフローチャートである。

[図5]第1実施形態における暗号化手順を示すフローチャートである。

[図6]第1実施形態における復号化手順を示すフローチャートである。

[図7]本発明の第2実施形態による暗号化／復号化装置の機能的構成を示すブロック図である。

[図8]第2実施形態における鍵生成手順を示すフローチャートである。

[図9]第2実施形態における暗号化手順を示すフローチャートである。

[図10]第2実施形態における復号化手順を示すフローチャートである。

符号の説明

[0087]

100 暗号化装置
101 平文入力装置
102 OAEP＋変換部
103 変換関数Aによる変換部
104 NTRU暗号化部
105 暗号文出力装置
200 復号化装置
201 暗号文入力装置
202 NTRU復号化部
203 乱数復元部
204 変換関数Aの逆変換部
205 OAEP＋逆変換部
206 平文出力装置
300 鍵生成装置
301 公開情報記憶装置
302 秘密鍵記憶装置

請求の範囲

[1] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用する方法において、

入力情報を前記パディング方式により所定長以下のビット列に変換し、

前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換し、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給し、

前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、

ことを特徴とするパディング適用方法。

[2] 前記変換規則は、前記ビット列の前半を前記第1ビット列とし、後半を前記第2ビット列とするように前記ビット列を2分割する規則であることを特徴とする請求項1に記載のパディング適用方法。

[3] 前記パディング方式はOAEP＋パディングであり、前記乱数を使用する暗号化方式はNTRU暗号方式であることを特徴とする請求項1または2に記載のパディング適用方法。

[4] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用する方法において、

入力情報を前記パディング方式により所定長以下のビット列に変換するパディング変換手段と、

前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換するビット列変換手段と、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して暗号文を生成する暗号化手段と、

前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、

ことを特徴とするパディング装置。

[5] 前記変換規則は、前記ビット列の前半を前記第1ビット列とし、後半を前記第2ビット列とするように前記ビット列を2分割する規則であることを特徴とする請求項4に記載のパディング装置。

[6] 前記パディング方式はOAEP＋パディングであり、前記乱数を使用する暗号化方式はNTRU暗号方式であることを特徴とする請求項4または5に記載のパディング装置。

[7] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用することで暗号文を生成する暗号化装置において、

入力した平文を前記パディング方式により所定長以下のビット列に変換するパディング変換手段と、

前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換するビット列変換手段と、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して暗号文を生成する暗号化手段と、

前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、

ことを特徴とする暗号化装置。

[8] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用することで暗号文を生成する暗号化装置において、

秘密鍵暗号の鍵をランダムに選択し、前記秘密鍵暗号の鍵を用いて、入力した平文を秘密鍵暗号化することで第1暗号文を生成する第1暗号化手段と、

前記秘密鍵暗号の鍵を前記パディング方式により所定長以下のビット列に変換するパディング変換手段と、

前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換するビット列変換手段と、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して第2暗号文を生成する第2暗号化手段と、

前記第1暗号文および前記第2暗号文を暗号文として出力する暗号文出力手段と、

を有し、前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、

ことを特徴とする暗号化装置。

[9] 前記変換規則は、前記ビット列の前半を前記第1ビット列とし、後半を前記第2ビット列とするように前記ビット列を2分割する規則であることを特徴とする請求項7または8に記載の暗号化装置。

[10] 前記パディング方式はOAEP＋パディングであり、前記乱数を使用する暗号化方式はNTRU暗号方式であることを特徴とする請求項7または8に記載の暗号化装置。

[11] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用することで暗号文を生成する方法において、

入力した平文を前記パディング方式により所定長以下のビット列に変換し、

前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換し、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して暗号文を生成し、

前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、

ことを特徴とする暗号化方法。

[12] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式に対して、乱数を使用しない暗号化方式で安全性が保証されたパディング方式を適用することで暗号文を生成する方法において、

秘密鍵暗号の鍵をランダムに選択し、

前記秘密鍵暗号の鍵を用いて、入力した平文を秘密鍵暗号化することで第1暗号文を生成し、

前記秘密鍵暗号の鍵を前記パディング方式により所定長以下のビット列に変換し、

前記ビット列を所定の変換規則によって第1ビット列と第2ビット列とに変換し、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して第2暗号文を生成し、

前記第1暗号文および前記第2暗号文を暗号文として出力し、

前記変換規則は、前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす、

ことを特徴とする暗号化方法。

[13] 前記変換規則は、前記ビット列の前半を前記第1ビット列とし、後半を前記第2ビット列とするように前記ビット列を2分割する規則であることを特徴とする請求項11または12に記載の暗号化方法。

[14] 前記パディング方式はOAEP＋パディングであり、前記乱数を使用する暗号化方式はNTRU暗号方式であることを特徴とする請求項11または12に記載の暗号化方法。

[15] 請求項7に記載の暗号化装置により生成された暗号文を復号化する装置において

、

前記乱数を使用する暗号化方式に対応する復号化方式に従って、入力した暗号文を復号化して第1ビット列を生成する第1復号化手段と、

前記暗号化に使用した乱数を第2ビット列として復元する乱数復号手段と、

前記変換規則の逆変換規則に従って、前記第1ビット列および前記第2ビット列を所定長以下のビット列に逆変換するビット列逆変換手段と、

前記所定長以下のビット列から前記パディング方式によるパディングを除去することで元の平文を生成するパディング逆変換手段と、

前記パディングの正当性を判断し、正当であれば前記平文を出力する判定手段と

、

を有することを特徴とする復号化装置。

[16] 請求項8に記載の暗号化装置により生成された暗号文を復号化する装置において

、

前記乱数を使用する暗号化方式に対応する復号化方式に従って、前記第2暗号文を復号化して第1ビット列を生成する第1復号化手段と、

前記暗号化に使用した乱数を第2ビット列として復元する乱数復号手段と、

前記変換規則の逆変換規則に従って、前記第1ビット列および前記第2ビット列を所定長以下のビット列に逆変換するビット列逆変換手段と、

前記所定長以下のビット列から前記パディング方式によるパディングを除去することで元の秘密鍵暗号の鍵を生成するパディング逆変換手段と、

前記パディングの正当性を判断し、正当であれば前記秘密鍵暗号の鍵を用いて前記第1暗号文を復号する第2復号手段と、

を有することを特徴とする復号化装置。

[17] 請求項11に記載の暗号化方法により生成された暗号文を復号化する方法において、

前記乱数を使用する暗号化方式に対応する復号化方式に従って、入力した暗号文を復号化して第1ビット列を生成し、

前記暗号化に使用した乱数を第2ビット列として復元し、

前記変換規則の逆変換規則に従って、前記第1ビット列および前記第2ビット列を所定長以下のビット列に逆変換し、

前記所定長以下のビット列から前記パディング方式によるパディングを除去することで元の平文を生成し、

前記パディングの正当性を判断し、正当であれば前記平文を出力する、

ことを特徴とする復号化方法。

[18] 請求項12に記載の暗号化方法により生成された暗号文を復号化する方法において、

前記乱数を使用する暗号化方式に対応する復号化方式に従って、前記第2暗号文を復号化して第1ビット列を生成し、

前記暗号化に使用した乱数を第2ビット列として復元し、

前記変換規則の逆変換規則に従って、前記第1ビット列および前記第2ビット列を所定長以下のビット列に逆変換し、

前記所定長以下のビット列から前記パディング方式によるパディングを除去することで元の秘密鍵暗号の鍵を生成し、

前記パディングの正当性を判断し、正当であれば前記秘密鍵暗号の鍵を用いて前記第1暗号文を復号する、

ことを特徴とする復号化方法。

[19] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式と、乱数を使用しない暗号化方式で安全性が保証されたパディング方式とを用い、通信ネットワークを通して通信端末間で暗号通信を行うシステムにおいて、

送信側通信端末は、

入力した平文を前記パディング方式により所定長以下のビット列に変換するパディング変換手段と、

前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像およびその逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす変換規則に従って、前記ビッ

ト列を第1ビット列と第2ビット列とに変換するビット列変換手段と、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して暗号文を生成する暗号化手段と、

前記暗号文を受信側端末へ送信する送信手段と、

を有し、

前記受信側通信端末は、

前記暗号文を前記送信側通信端末から受信する受信手段と、

前記乱数を使用する暗号化方式に対応する復号化方式に従って、入力した暗号文を復号化して第1ビット列を生成する第1復号化手段と、

前記暗号化に使用した乱数を第2ビット列として復元する乱数復号手段と、

前記変換規則の逆変換規則に従って、前記第1ビット列および前記第2ビット列を所定長以下のビット列に逆変換するビット列逆変換手段と、

前記所定長以下のビット列から前記パディング方式によるパディングを除去することで元の平文を生成するパディング逆変換手段と、

前記パディングの正当性を判断し、正当であれば前記平文を出力する判定手段と、

を有する、

ことを特徴とする暗号通信システム。

[20] 暗号文の作成に乱数を使用し、その使用した乱数を受信側で復元できる暗号化方式と、乱数を使用しない暗号化方式で安全性が保証されたパディング方式とを用い、通信ネットワークを通して通信端末間で暗号通信を行うシステムにおいて、

送信側通信端末は、

秘密鍵暗号の鍵をランダムに選択し、前記秘密鍵暗号の鍵を用いて、入力した平文を秘密鍵暗号化することで第1暗号文を生成する第1暗号化手段と、

前記秘密鍵暗号の鍵を前記パディング方式により所定長以下のビット列に変換するパディング変換手段と、

前記所定長以下のビット列を前記第1ビット列の集合と第2ビット列の集合との直積の元に対応させる写像であり、かつ、前記写像は単射であること、前記写像および

その逆写像が多項式時間で計算可能であること、および、前記直積を定義域とする前記暗号化関数が一方向性関数であること、を満たす変換規則に従って、前記ビット列を第1ビット列と第2ビット列とに変換するビット列変換手段と、

前記第1ビット列をデータ入力とし、前記第2ビット列を乱数入力として暗号化関数にそれぞれ供給して第2暗号文を生成する第2暗号化手段と、

前記第1暗号文および前記第2暗号文を暗号文として出力する暗号文出力手段と、

を有し、

前記受信側通信端末は、

前記暗号文を前記送信側通信端末から受信する受信手段と、

前記乱数を使用する暗号化方式に対応する復号化方式に従って、前記第2暗号文を復号化して第1ビット列を生成する第1復号化手段と、

前記暗号化に使用した乱数を第2ビット列として復元する乱数復号手段と、

前記変換規則の逆変換規則に従って、前記第1ビット列および前記第2ビット列を所定長以下のビット列に逆変換するビット列逆変換手段と、

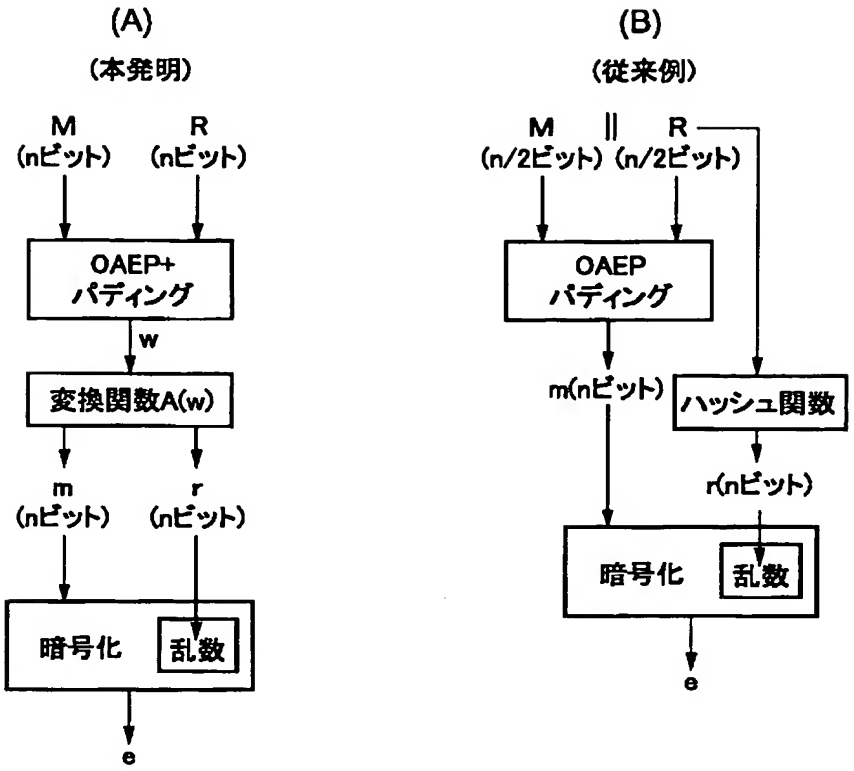
前記所定長以下のビット列から前記パディング方式によるパディングを除去することで元の秘密鍵暗号の鍵を生成するパディング逆変換手段と、

前記パディングの正当性を判断し、正当であれば前記秘密鍵暗号の鍵を用いて前記第1暗号文を復号する第2復号手段と、

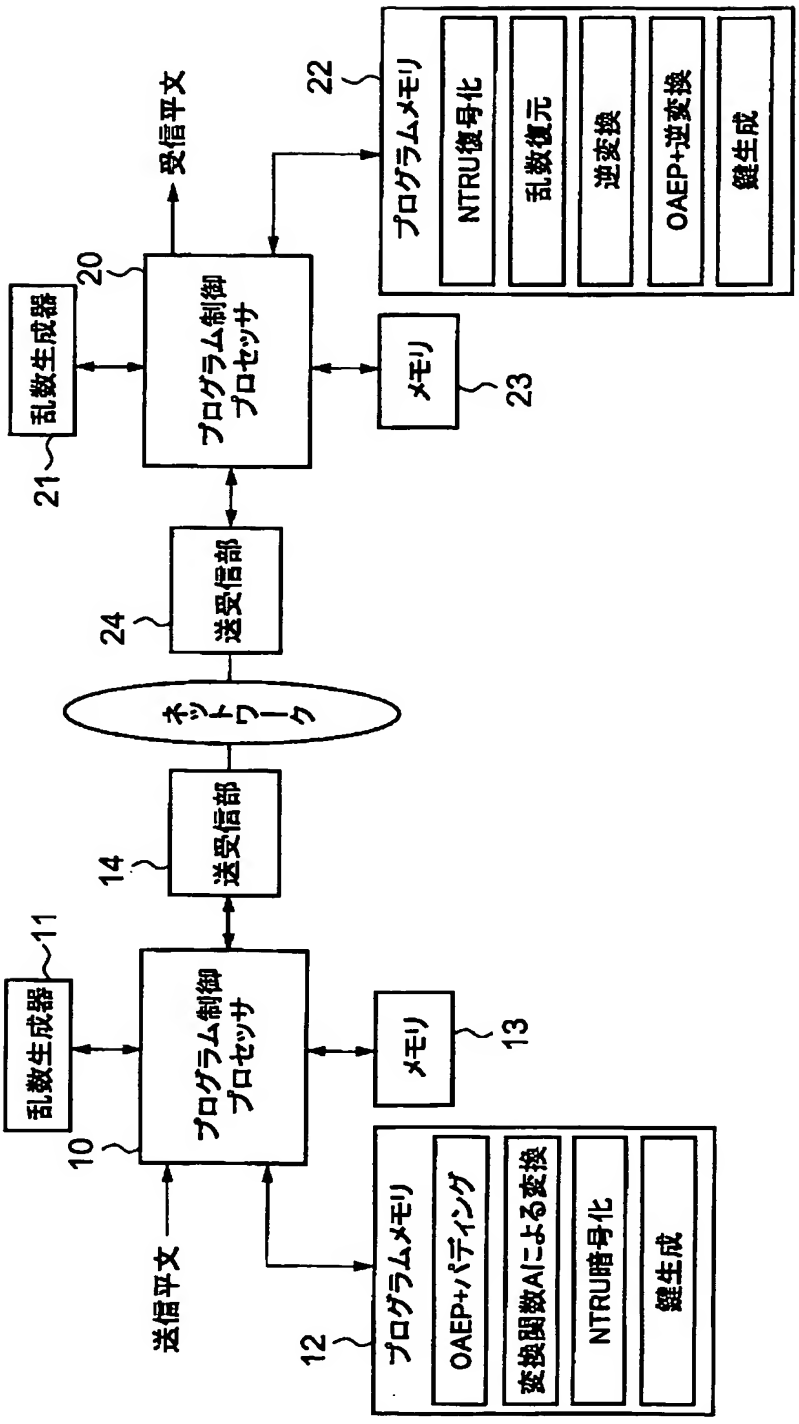
を有する、

ことを特徴とする暗号通信システム。

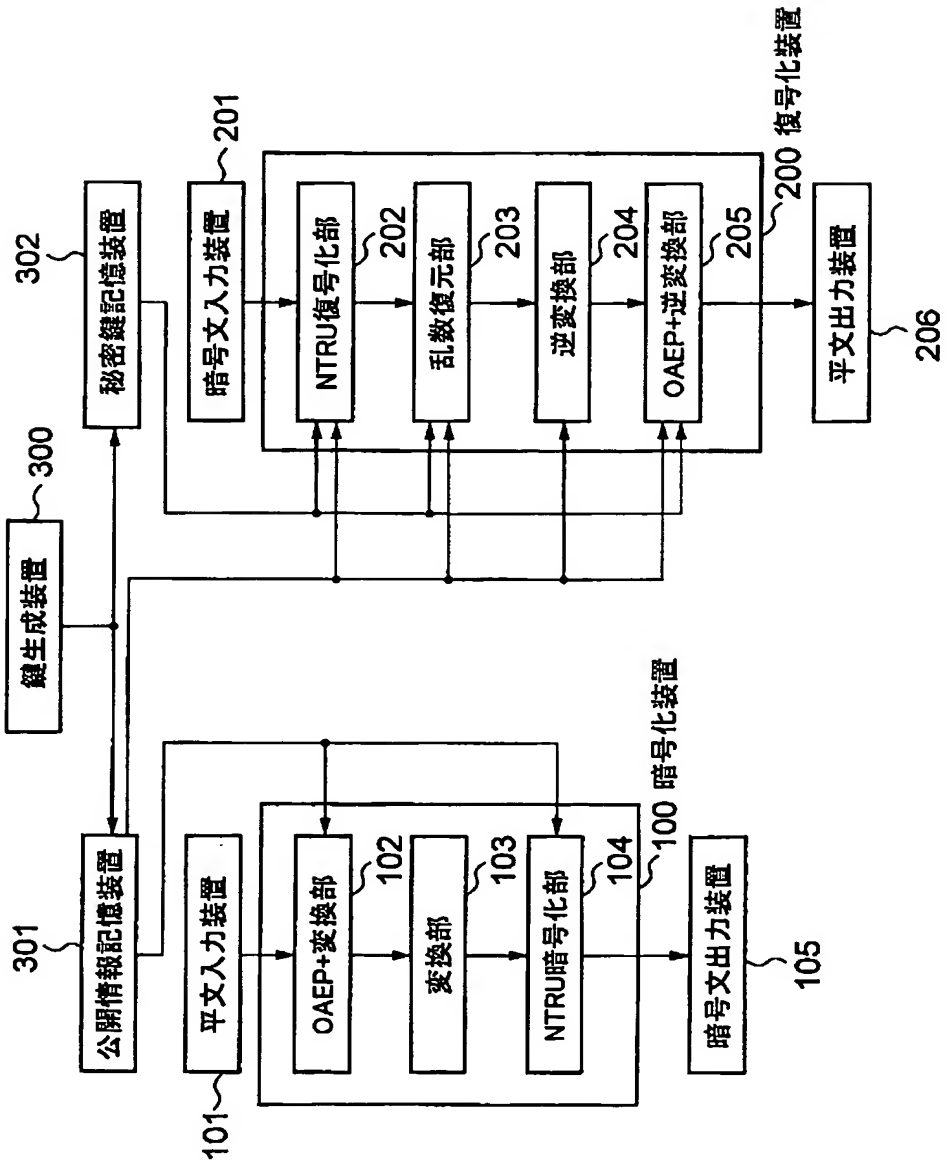
[図1]


(A)
(本発明)
M
(nビット)
R
(nビット)
OAEP+
パディング
w
変換関数A(w)
m
(nビット)
r
(nビット)
暗号化
乱数
e
(B)
(従来例)
M
(n/2ビット)
R
(n/2ビット)
OAEP
パディング
m(nビット)
ハッシュ関数
r(nビット)
暗号化
乱数
e

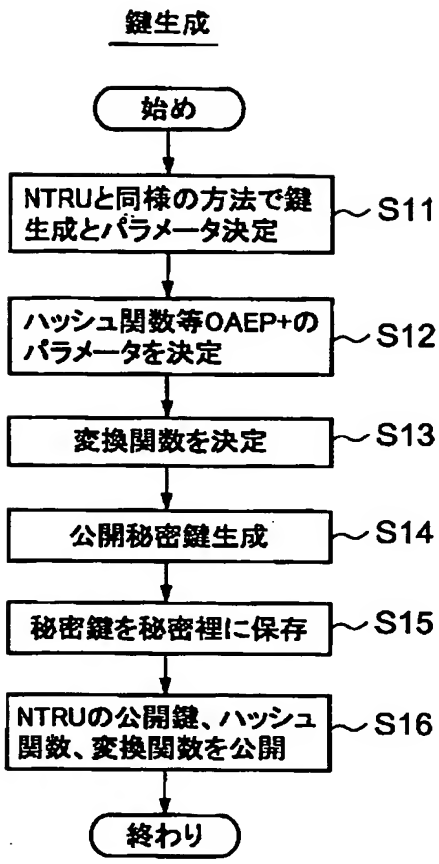
[図2]


送信平文
10
プログラム制御プロセッサ
11
乱数生成器
メモリ
13
プログラムメモリ
12
OAEP+パディング
変換関数AIによる変換
NTRU暗号化
鍵生成
送受信部
14
ネットワーク
送受信部
24
プログラム制御プロセッサ
20
乱数生成器
21
メモリ
23
プログラムメモリ
22
NTRU復号化
乱数復元
逆変換
OAEP+逆変換
鍵生成
受信平文

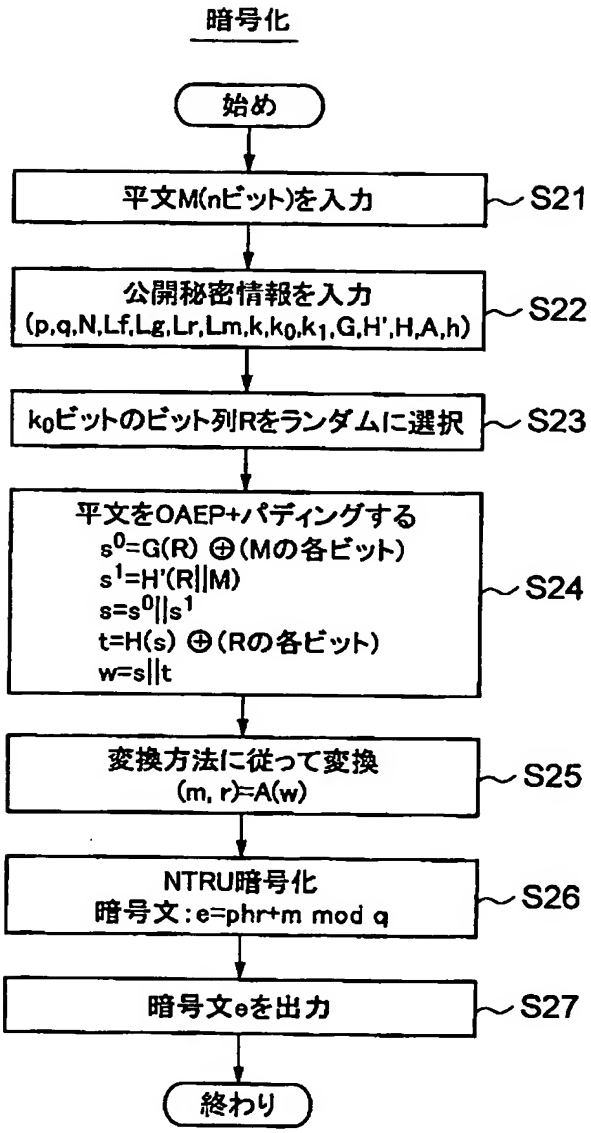
[図3]


鍵生成装置
300
秘密鍵記憶装置
302
公開情報記憶装置
301
暗号文入力装置
201
平文入力装置
101
NTRU復号化部
202
乱数復元部
203
逆変換部
204
OAEP+逆変換部
205
復号化装置
200
平文出力装置
206
OAEP+変換部
102
変換部
103
NTRU暗号化部
104
暗号化装置
100
暗号文出力装置
105

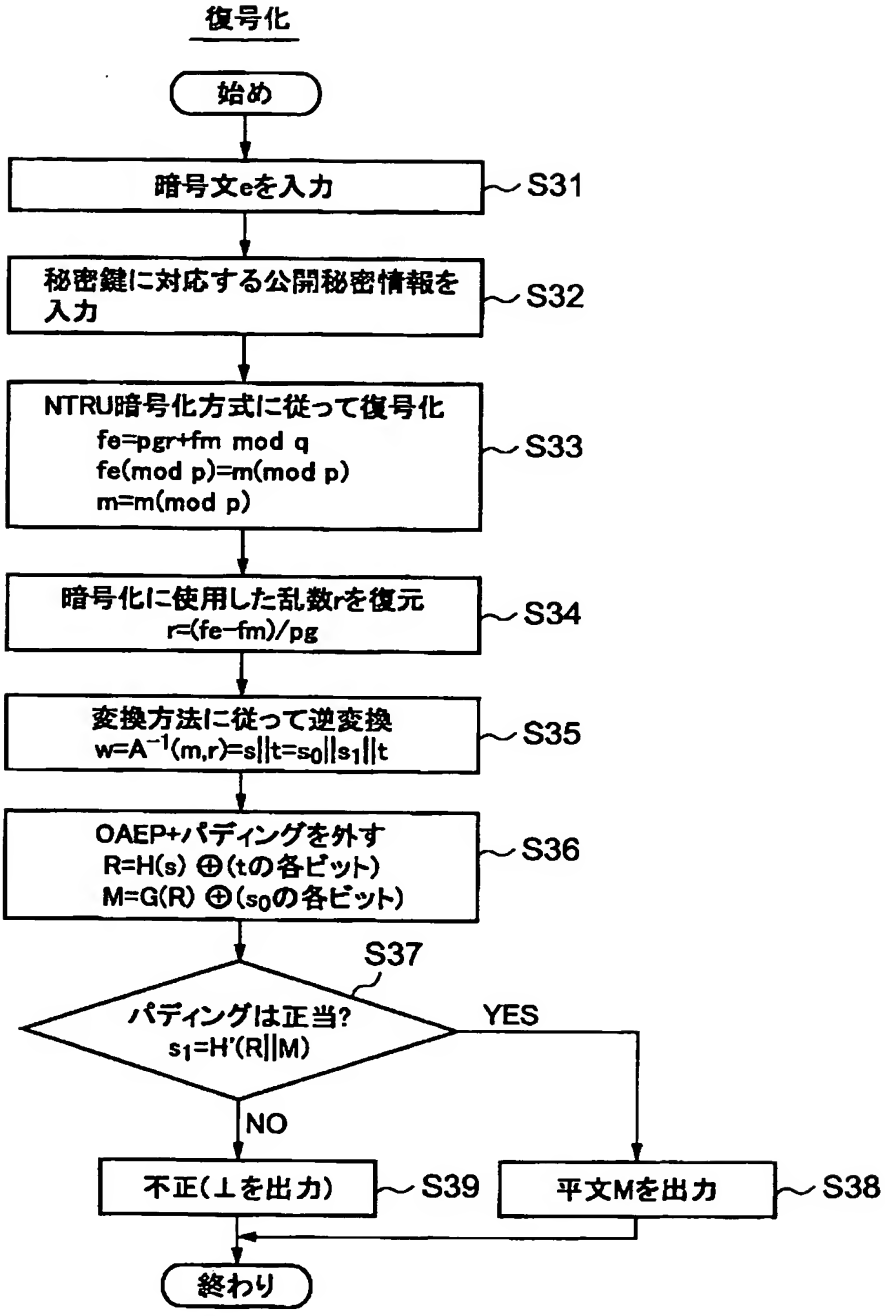
[図4]


鍵生成
始め
NTRUと同様の方法で鍵生成とパラメータ決定
S11
ハッシュ関数等OAEP+のパラメータを決定
S12
変換関数を決定
S13
公開秘密鍵生成
S14
秘密鍵を秘密裡に保存
S15
NTRUの公開鍵、ハッシュ関数、変換関数を公開
S16
終わり

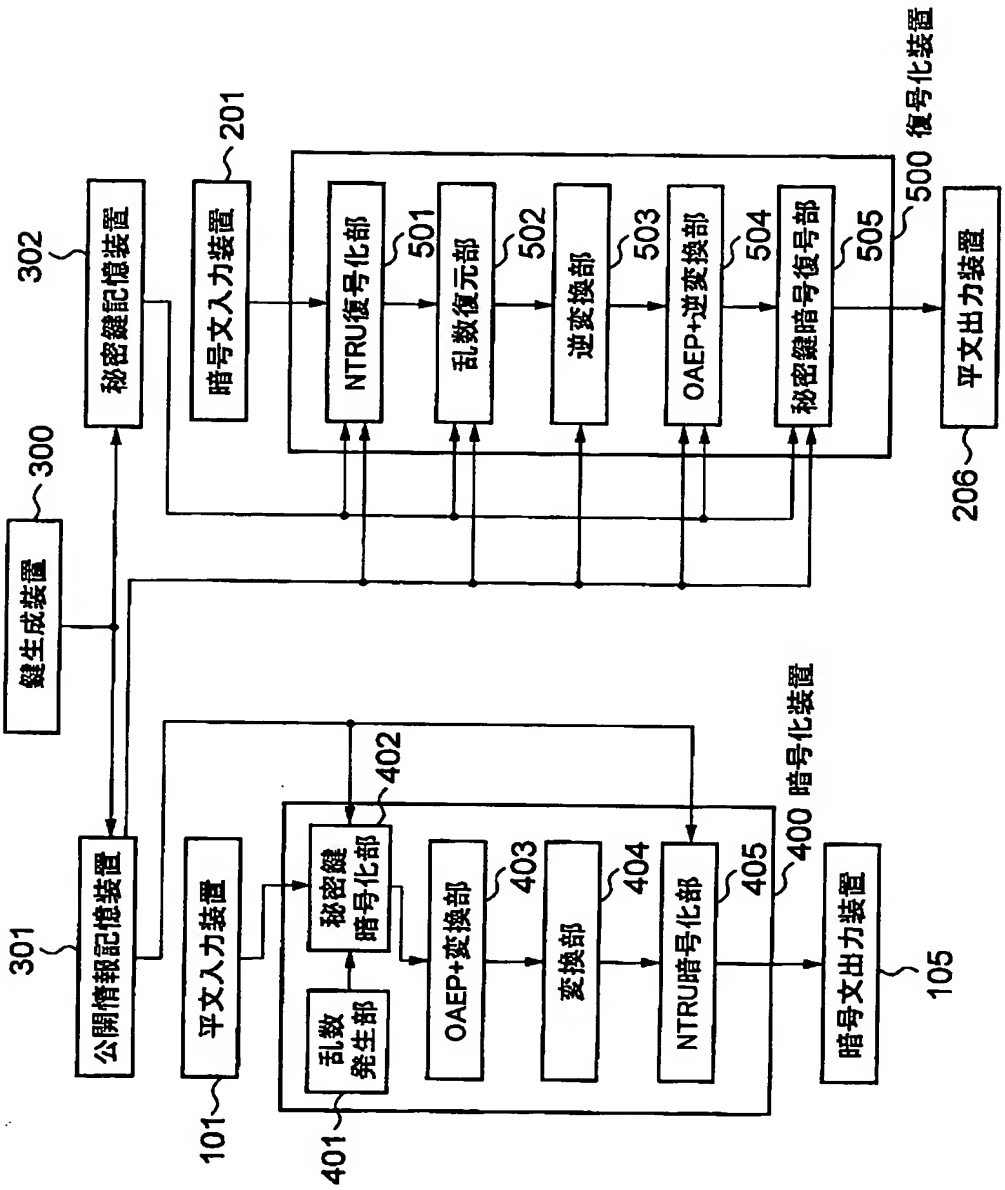
[図5]


暗号化
始め
平文M(nビット)を入力
S21
公開秘密情報を入力
(p,q,N,Lf,Lg,Lr,Lm,k,k0,k1,G,H',H,A,h)
S22
k0ビットのビット列Rをランダムに選択
S23
平文をOAEP+パディングする
s0=G(R) ⊕(Mの各ビット)
s1=H'(R||M)
s=s0||s1
t=H(s) ⊕(Rの各ビット)
w=s||t
S24
変換方法に従って変換
(m, r)=A(w)
S25
NTRU暗号化
暗号文:e=phr+m mod q
S26
暗号文eを出力
S27
終わり

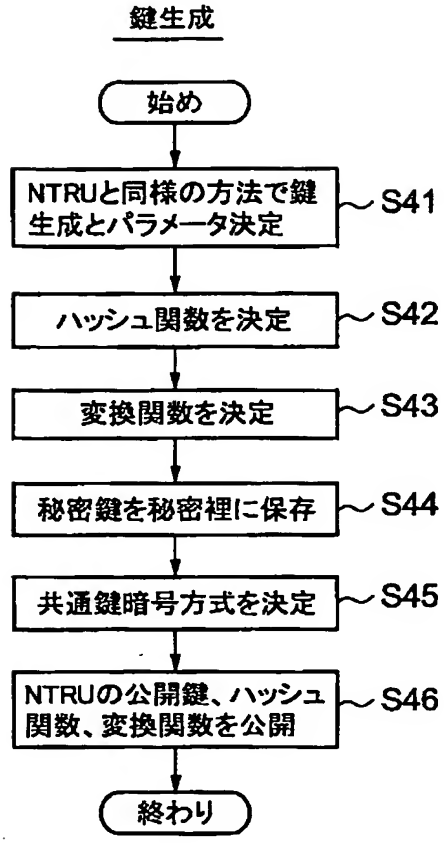
[図6]


復号化
始め
暗号文eを入力
S31
秘密鍵に対応する公開秘密情報を入力
S32
NTRU暗号化方式に従って復号化
fe=pgr+fm mod q
fe(mod p)=m(mod p)
m=m(mod p)
S33
暗号化に使用した乱数rを復元
r=(fe−fm)/pg
S34
変換方法に従って逆変換
w=A^-1(m,r)=s||t=s0||s1||t
S35
OAEP+パディングを外す
R=H(s) ⊕(tの各ビット)
M=G(R) ⊕(s0の各ビット)
S36
S37
パディングは正当?
s1=H'(R||M)
YES
NO
不正(⊥を出力)
S39
平文Mを出力
S38
終わり

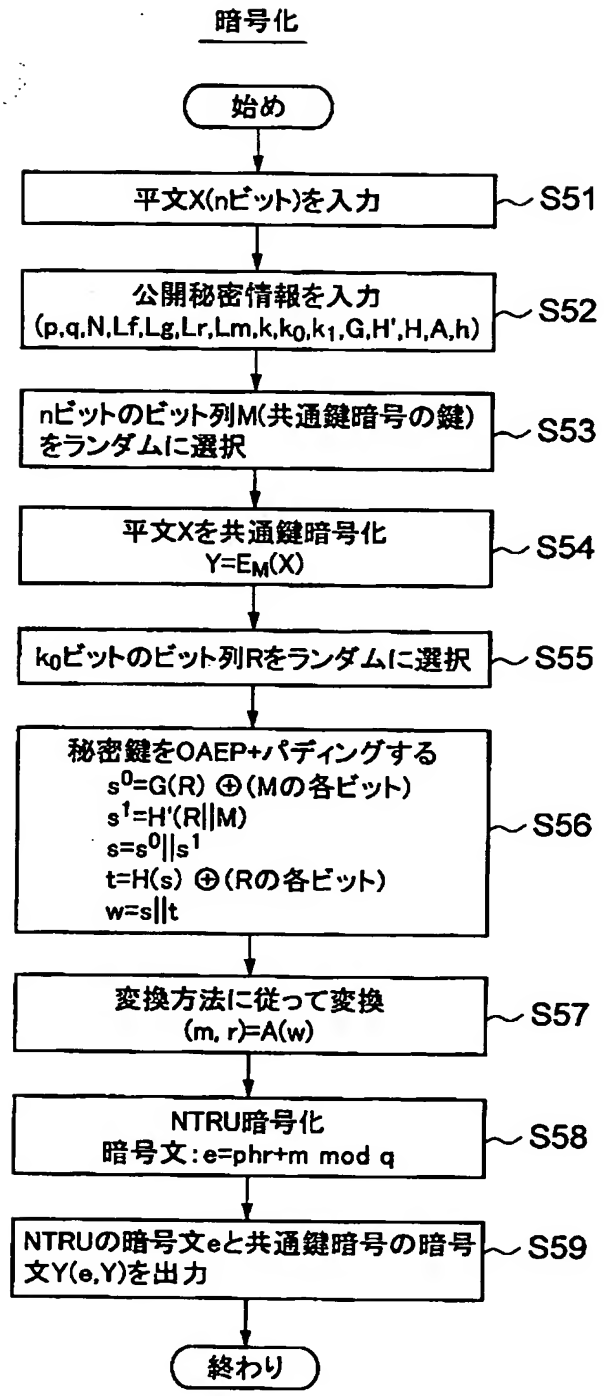
[図7]


鍵生成装置
300
公開情報記憶装置
301
秘密鍵記憶装置
302
平文入力装置
101
暗号文入力装置
201
乱数発生部
401
秘密鍵暗号化部
402
OAEP+変換部
403
変換部
404
NTRU暗号化部
405
暗号化装置
400
暗号文出力装置
105
NTRU復号化部
501
乱数復元部
502
逆変換部
503
OAEP+逆変換部
504
秘密鍵暗号復号部
505
復号化装置
500
平文出力装置
206

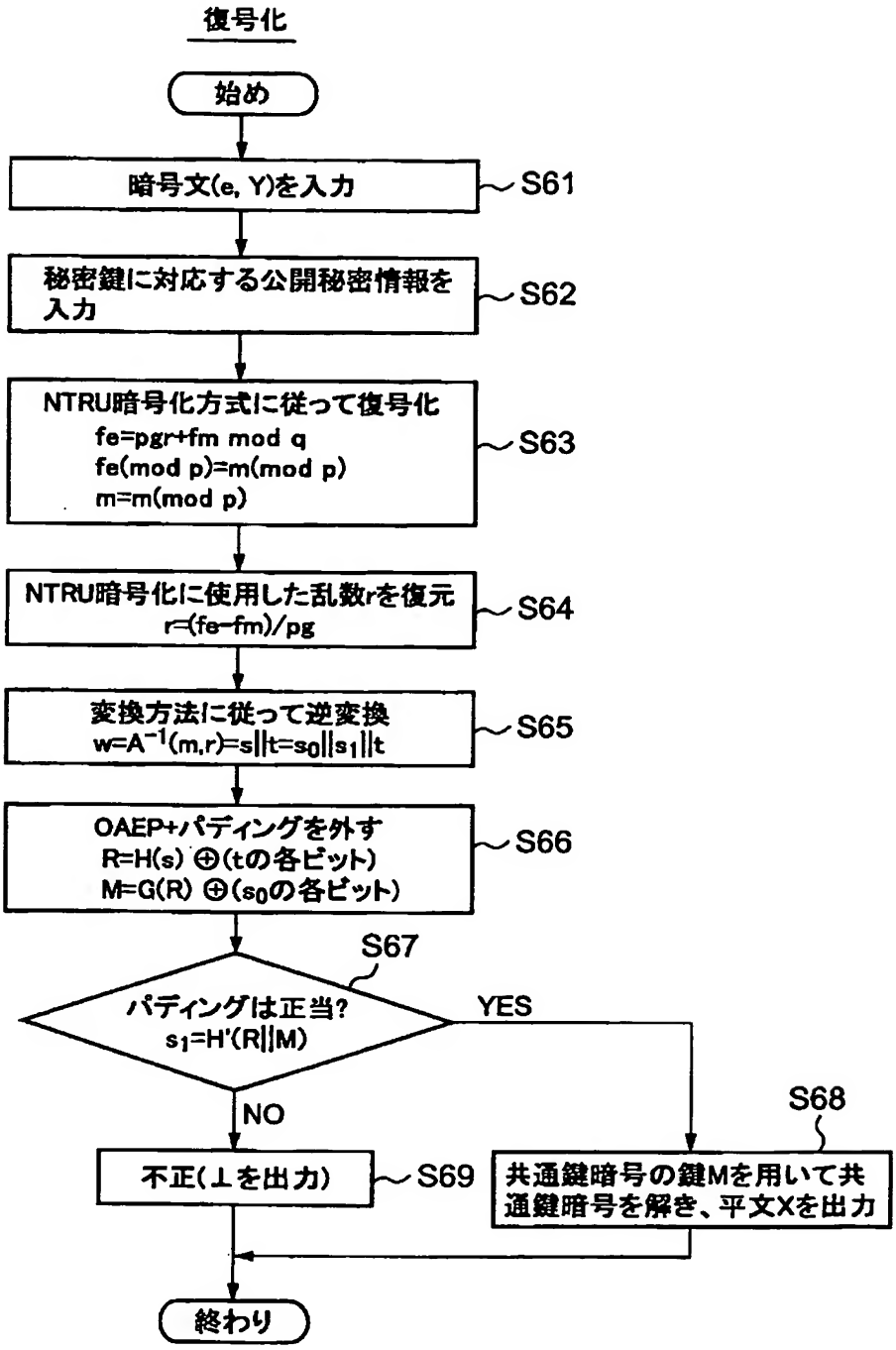
[図8]


鍵生成
始め
NTRUと同様の方法で鍵生成とパラメータ決定
S41
ハッシュ関数を決定
S42
変換関数を決定
S43
秘密鍵を秘密裡に保存
S44
共通鍵暗号方式を決定
S45
NTRUの公開鍵、ハッシュ関数、変換関数を公開
S46
終わり

[図9]


暗号化
始め
平文X(nビット)を入力
S51
公開秘密情報を入力
(p,q,N,Lf,Lg,Lr,Lm,k,k0,k1,G,H',H,A,h)
S52
nビットのビット列M(共通鍵暗号の鍵)をランダムに選択
S53
平文Xを共通鍵暗号化
Y=EM(X)
S54
k0ビットのビット列Rをランダムに選択
S55
秘密鍵をOAEP+パディングする
s0=G(R) ⊕(Mの各ビット)
s1=H'(R||M)
s=s0||s1
t=H(s) ⊕(Rの各ビット)
w=s||t
S56
変換方法に従って変換
(m, r)=A(w)
S57
NTRU暗号化
暗号文:e=phr+m mod q
S58
NTRUの暗号文eと共通鍵暗号の暗号文Y(e,Y)を出力
S59
終わり

[図10]


復号化
始め
暗号文(e, Y)を入力
S61
秘密鍵に対応する公開秘密情報を入力
S62
NTRU暗号化方式に従って復号化
fe=pgr+fm mod q
fe(mod p)=m(mod p)
m=m(mod p)
S63
NTRU暗号化に使用した乱数rを復元
r=(fe-fm)/pg
S64
変換方法に従って逆変換
w=A^-1(m,r)=s||t=s0||s1||t
S65
OAEP+パディングを外す
R=H(s) ⊕(tの各ビット)
M=G(R) ⊕(s0の各ビット)
S66
S67
パディングは正当?
s1=H'(R||M)
YES
NO
S68
不正(⊥を出力)
S69
共通鍵暗号の鍵Mを用いて共通鍵暗号を解き、平文Xを出力
終わり

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/005287

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus FILE(JOIS), NTRU, OAEP

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SHOUP V., OAEP Reconsidered (Extended Abstract), LNCS, Vol.2139, 2001, pages 239 to 259	1-20
A	NGUYEN P.Q., POINTCHEVAL D., Analysis and Improvements of NTRU Encryption Paddings, LNCS, Vol.2442, 2002, pages 210 to 225	1-20
A	JP 2000-516733 A (NTRU Cryptosystems, Inc.), 12 December, 2000 (12.12.00), Full text & US 6081597 A & EP 920753 A & WO 1998/8323 A1 & AU 4582897 A & CA 2263588 A & CN 1232588 A	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 April, 2005 (20.04.05)	17 May, 2005 (17.05.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号 PCT／JP2005／005287

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl.[7] G09C1/00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl.[7] G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2005年
日本国実用新案登録公報	1996－2005年
日本国登録実用新案公報	1994－2005年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlusファイル(JOIS), NTRU, OAEP

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	SHOUP V, OAEP Reconsidered (Extended Abstract), LNCS, Vol. 2139, 2001, p. 239-259	1-20
A	NGUYEN P Q, POINTCHEVAL D, Analysis and Improvements of NTRU Encryption Paddings, LNCS, Vol. 2442, 2002, p. 210-225	1-20

☑ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 20. 04. 2005	国際調査報告の発送日 17.05.2005
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 5M 3365 石田 信行 電話番号 03－3581－1101 内線 3599

様式PCT／ISA／210（第2ページ）（2004年1月）

国際調査報告

国際出願番号 PCT／JP2005／005287

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 2000-516733 A（エヌティーアールユー クリプトシステムズ，インコーポレーテッド）2000.12.12，全文 & US 6081597 A & EP 920753 A & WO 1998/8323 A1 & AU 4582897 A & CA 2263588 A & CN 1232588 A	1-20

様式PCT／ISA／210（第2ページの続き）（2004年1月）